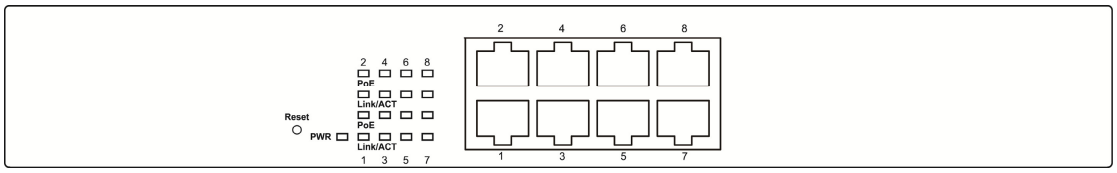
User Manual



8-Port 10/100/1000Mbps with 8-port PoE+

Web Management Switch

Content

Content **2**

Introduction **4**

Product Overview 4

Web Management Features 4

Specifications 5

Mechanical 5

Performance 5

Package Contents 6

Hardware Description **7**

Physical Dimensions/ Weight 7

Front Panel 7

LED Indicators 7

Rear Panel 8

Hardware Installation 8

Software Description **9**

Configuration 10

System 10

Ports 12

VLAN 13

Aggregation 16

RSTP 17

IGMP Snooping 19

Mirroring 20

Quality of Service (QoS) 21

PoE (Power over Ethernet) Configuration 24

Storm Control 25
Monitoring 26
Statistic Overview 26
Detailed Statics 27
RSTP Status 27
IGMP Status 28
Ping 29
Maintenance 31
Warm Restart 31
Factory Default 31
Software upload 31
Configuration File Transfer 32
Logout 32
Reset button for the factory default setting 33

Introduction

Product Overview

This switch is a Web Smart Switch equipped with 8-ports 10/100/1000BaseT(X) with 8 PoE+ Ports. It is designed for easy installation and high performance in an environment where traffic is on the network and the number of users increased continuously. The compact rigid 19" rack-mount size is specifically designed for small to medium workgroups. It can be installed where space is limited; moreover, it provides smooth network migration and is easy to upgrade the network capacity.

In addition, the switch features comprehensive and useful functions, such as: QoS (Quality of Service), Spanning Tree, VLAN, Power over Ethernet (PoE), Static Link Aggregation, SNMP/RMON, IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

Web Management Features

- Configuration
  - System
  - Ports
  - VLANs
  - Aggregation
  - RSTP
  - IGMP Snooping
  - Mirroring
  - Quality of Service
  - Power over Ethernet
  - Storm Control
- Monitoring
  - Statistics Overview
  - Detailed Statistics
  - RSTP Status
  - IGMP Status
  - Ping

- Maintenance
  Warm Restart
  Factory Default
  Software Upload
  Configuration File Transfer
  Logout

Specifications

- Standard
  IEEE 802.3 10BaseT
  IEEE 802.3u 100BaseTX
  IEEE 802.3ab 1000BaseT
  IEEE 802.3af PoE
  IEEE 802.3at PoE^{+}
  IEEE 802.3z 1000BaseSX/LX
  IEEE 802.3x Full-duplex Flow Control
  IEEE 802.1Q VLAN
  IEEE 802.1d Spanning tree protocol
  IEEE 802.1w Rapid Spanning tree protocol
  IEEE 802.1p QoS

- Number of Port
  8-port 10/100/1000BaseT(X) with 8-port PoE+

Mechanical

- LED Indicator
  Port 1~8: Link/ ACT
  Port 1~8: PoE
  Per Unit: Power

- Power Consumption: 250 Watts (Max), 30 Watts per port

- Power Input: 100~240V/AC, 50~60HZ
  Product Dimensions/ Weight: 266 × 160 × 44 mm (L × W ×H) / 1.6kg

Performance

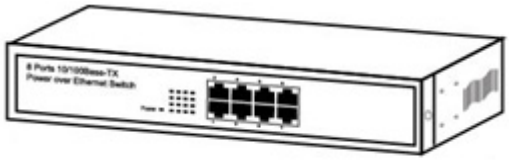
- MAC Address & Multicast group: 8K
- Buffer Memory: 176 KB
- Jumbo Frames: 9.6K

➢ Transmission Method: Store and Forward

Package Contents

Before you start to install this switch, please verify your package that contains the following items:

- One PoE Gigabit Ethernet Switch
- One AC Power Cord
- One User Manual



Power Cord

Hardware Description

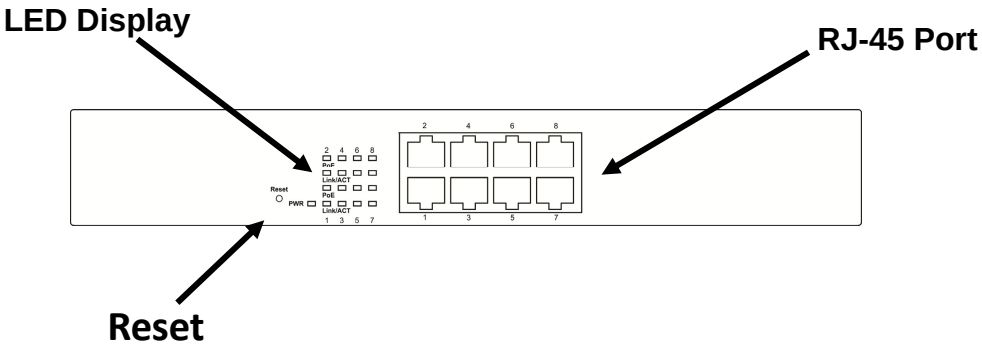
This part primarily presents hardware of this switch, physical dimensions and functional overview would be described.

Physical Dimensions/ Weight

266 × 160 × 44 mm (L × W ×H) / 1.6kg

Front Panel

The front Panel of the Web Smart Switch consists of 8 gigabit RJ-45 ports. The LED Indicators are also located on the front panel.

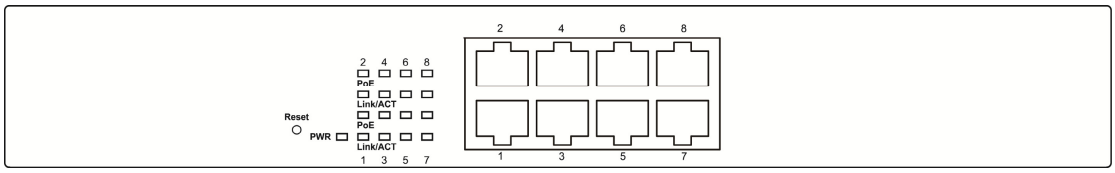


LED Indicators

The LED Indicators present real-time information of systematic operation status. The following table provides description of LED status and their meaning.

Table 1-1 LED Indicators

LED	Status	Description
Power	On	Power is on.
	Off	Power is off.
Link/ACT Port 1~8	On	10/100/1000 Link is connected.
	Blinking	Transmitting or receiving data.
PoE Port 1~8	On	Providing the power.
	Off	Not providing the power.



Rear Panel

The 3-pronged power plug is placed at the rear panel of the switch right side shown as below.

Hardware Installation

Set the switch on a large flat space with a power socket close by. The flat space should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation. The last, use twisted pair cable to connect this switch to your PC then user could start to operate the switch.

Software Description

This part instructs user how to set up and manage the switch through the web user interface. Please follow the description to understand the procedure.

At the first, open the web browser, and go to 192.168.2.1 site then the user will see the login screen. Just clicks the **Apply** then the login process is completed and comes out the sign “Password successfully entered”. The factory default password is “admin”.

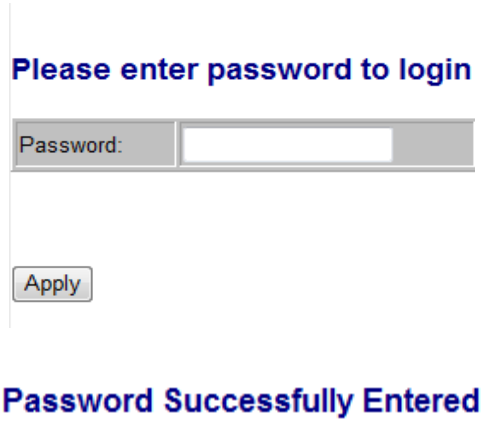


Figure 1-1

After the user login, the right side of website shows all functions as Fig. 1-2.

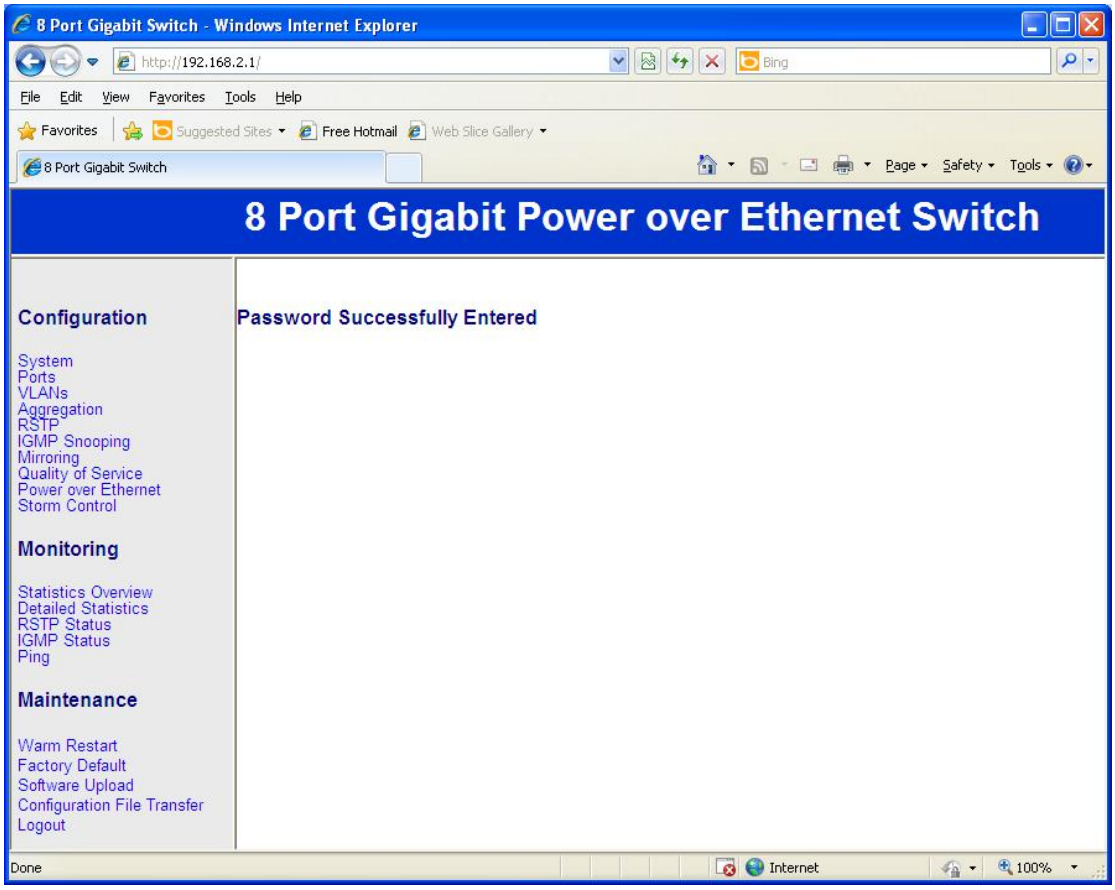


Figure 1-2

Configuration

System

System Configuration

This page shows system configuration information. User can configure lots of information as Fig. 1-3:

System Configuration

MAC Address	00-03-ce-09-1e-b4
S/W Version	V110915
H/W Version	1.0
Active IP Address	192.168.2.1
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.2.254
DHCP Server	0.0.0.0
Lease Time Left	0 secs

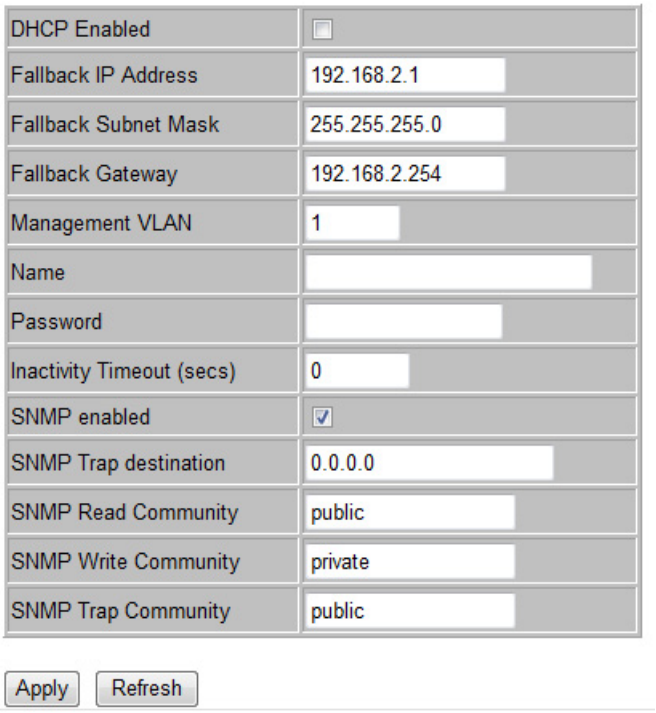


Figure 1-3

- MAC Address: Displays the unique hardware address assigned by manufacturer (default).
- S/W Version: Displays the switch's firmware version.
- H/W Version: Displays the switch's Hardware version.
- DHCP Enabled: Click the box to enable DHCP.
- Fallback IP address: Manually assign the IP address that the network is using. The default IP is 192.168.2.1.
- Fallback Subnet Mask: Assign the subnet mask to the IP address.
- Fallback Gateway: Assign the network gateway for industrial switch. The default gateway is 0.0.0.0.
- Management VLAN: ID of a configured VLAN (1-4096) through which you can manage the switch. By default, all ports on the switch are members of VLAN 1. However, if the management VLAN is changed, the management station must be attached to a port belonging to this VLAN.
- Name: Type in the new user name (The default value is 'admin').
- Password: Type in the new password (The default value is 'admin').
- Inactivity Timeout: Type in the inactivity timeout (60~10000 seconds).
- SNMP Enabled: Enables or disables SNMP on the switch. Supports SNMP version 1 and 2c management clients.
- SNMP Trap Destination: IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are

issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station.

- SNMP Read Community: A community string that acts like a password and permits access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects.
- SNMP Write Community: A community string that acts like a password and permits to write to the SNMP database on this switch.
- SNMP Trap Community: Community string sent with the notification operation.

Ports

Port Security ensures access to a switch port based on MAC address, limits the total number of devices from using a switch port, and protects against MAC flooding attacks.

Port Configuration

In Port Configuration, you can set and view the operation mode for each port.

- Enable Jumbo Frames: This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9.6 KB. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- Power Saving Mode: Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

- Mode: allow user to manually set the port speed such as Auto, 10 half, 10 Full, 100 Half, 100 Full, 1000 Full or Disabled. User may press Apply button to complete the configuration procedure.

- Flow Control: Enables or disables flow control for the port.

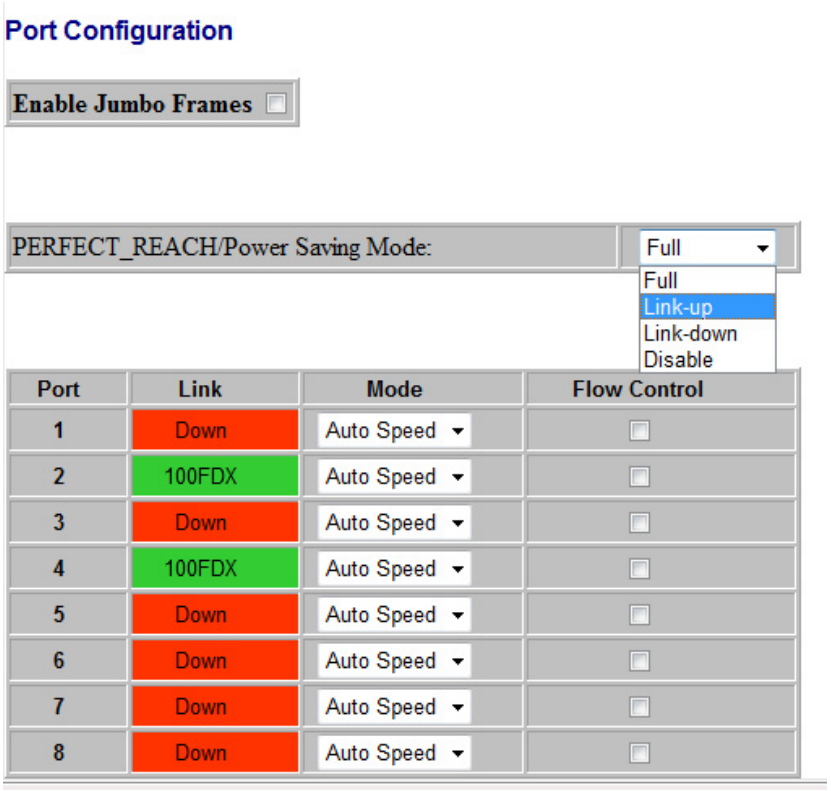


Figure 1-4-1

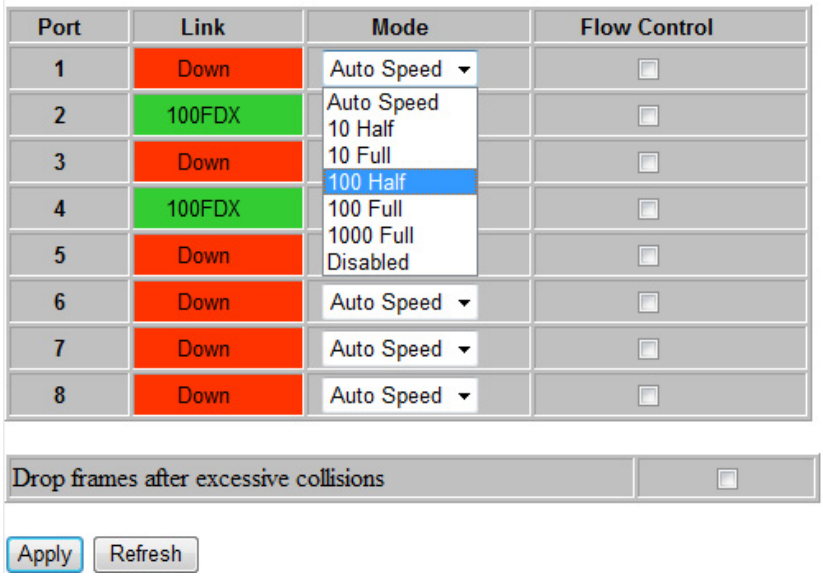


Figure 1-4-2

VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the ones of the same VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network

devices are still plugged into the same switch physically.

Port Segmentation (VLAN) Configuration

- VLAN ID: ID of configured VLAN (1-4096, no leading zeroes).
- VLAN Configuration List: Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

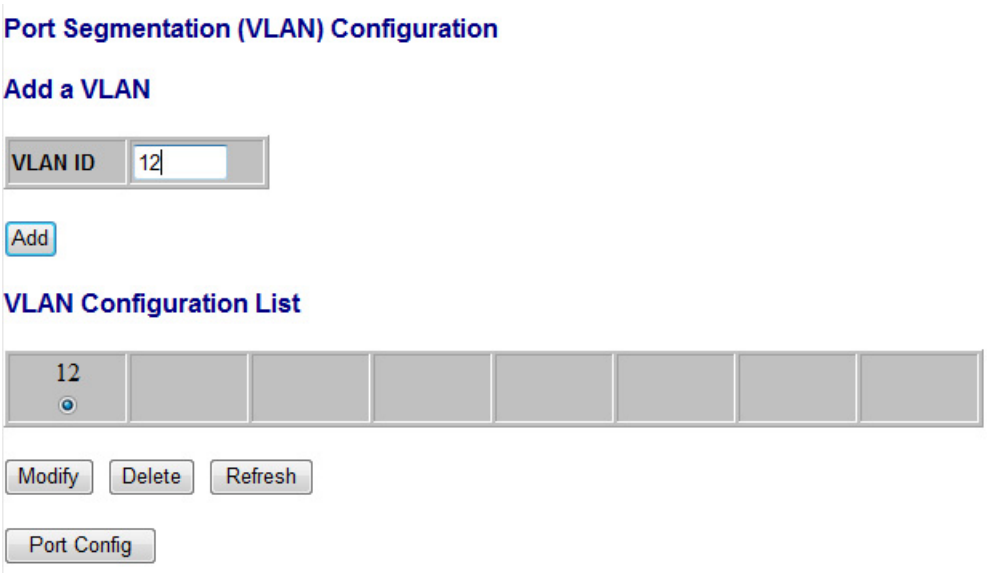


Figure 1-5-1

VLAN Setup

The switch supports up to 16 VLANs based on 802.1Q standard. From the VLAN Membership page you can create and delete VLANs, and change the VLAN port membership.

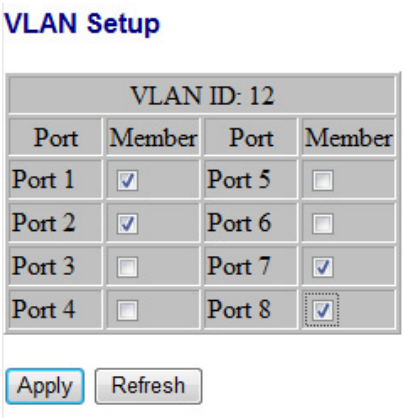


Figure 1-5-2

VLAN Per Port Configuration

The 802.1Q Per Port Configuration page allows you to change the VLAN parameters for individual ports or trunks. You can configure VLAN behavior for specific interfaces, including the accepted frame types and default VLAN identifier (PVID). Each row of the table corresponds to one port.

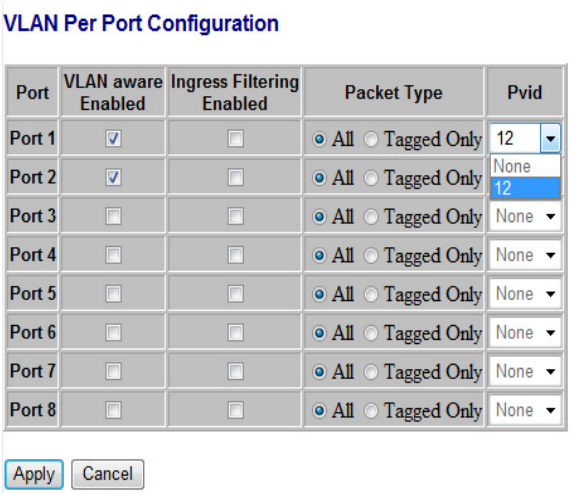


Figure 1-5-3

- Port: The port number of the port.
- VLAN Aware Enabled: VLAN aware ports are able to use VLAN tagged frames to determine the destination VLAN of a frame. (Default: Enabled) VLAN aware ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (except for the PVID). VLAN unaware ports will not strip the tag from received frames or insert the tag in transmitted frames.
- Ingress Filtering Enabled: If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded. (Default: Disabled)
- Packet Type: Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. (Default: All) If the Packet Type is set to “All”, the port can accept incoming tagged and untagged packets. Any received packets that are untagged are assigned to the default VLAN. Any tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. If the Packet Type is set to “Tagged Only”, the port will drop untagged packets and will only receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. Switches should be connected to each other with the Packet Type set to “Tagged Only”.
- PVID: The PVID (Port VLAN ID) is associated with untagged, ingress

packets. It is assigned to untagged frames received on the specified interface. The PVID has no effect on ports that have Packet Type set to “Tagged Only”. (Default PVID: 1) It is not possible to remove a port from VLAN 1 unless its PVID has been changed to something other than 1. Outgoing packets are tagged unless the packet’s VLAN ID is the same as the PVID. When the PVID is set to “None”, all outgoing packets are tagged.

※Note: If you select “Tagged Only” mode for a port, we recommend setting the PVID to “None” as the standard configuration.

Aggregation

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

Aggregation / Trunking Configuration

To assign a port to a trunk, click the required trunk number, and then click Apply.

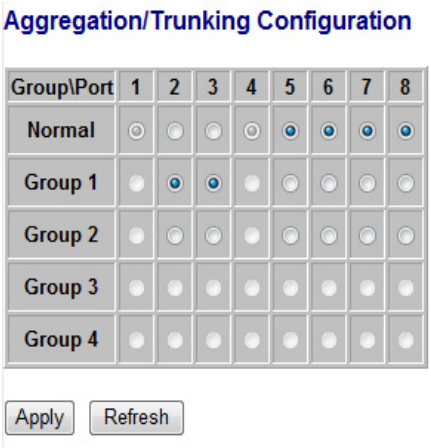


Figure 1-6

RSTP

IEEE 802.1w Rapid Spanning tree protocol (RSTP) provides a loop-free network and redundant links to the core network with rapid convergence to ensure faster recovery from failed links, enhancing overall network stability and reliability.

RSTP System Configuration

- System Priority: This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- Hello Time: Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1-10 (default is 2).
- Max Age – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6-40 (default is 20).
- Forward Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 – 30 (default is 15).
- Force Version: Set and show the RSTP protocol to use. Normal - use RSTP, Compatible - compatible with STP.

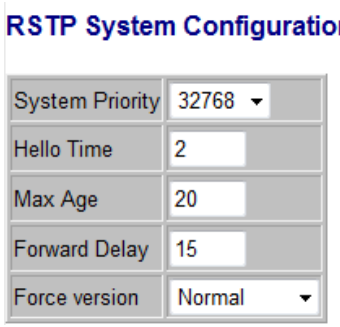


Figure 1-7-1

RSTP Port Configuration

- Port: The port ID. It cannot be changed. Aggregations mean any configured trunk group.
- Enabled: Click on the tick-box to enable/disable the RSTP protocol for the port.
- Edge: Expect the port to be an edge port (linking to an end station) or a link to another STP device.

- Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP path cost on the port. Number between 0 - 200000000. 0 means auto generated path cost.

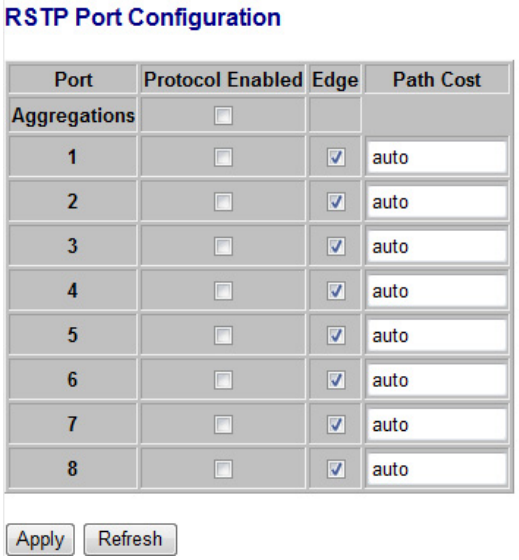


Figure 1-7-2

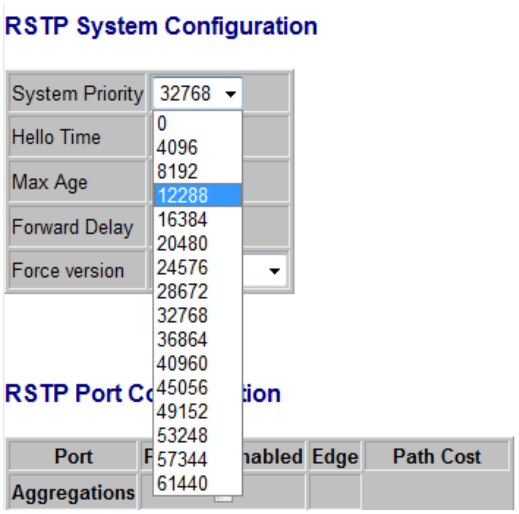


Figure 1-7-3

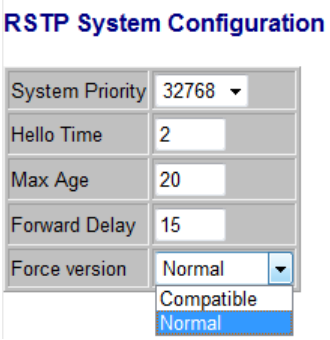


Figure 1-7-4

IGMP Snooping

IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer3 IGMP packets sent in a multicast network.

When IGMP Snooping is enabled in a switch it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

Prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to only the subscribers.

IGMP Configuration

- IGMP Enabled: When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
- Router Ports: Set if ports are connecting to the IGMP administrative routers.
- Unregistered IPMC Flooding enabled: Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.
- IGMP Snooping Enabled: When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.
- IGMP Querying Enabled: When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

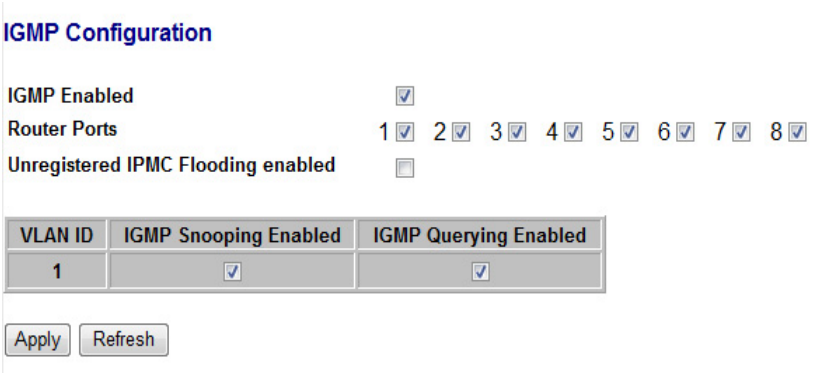


Figure 1-8

Mirroring

Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

Mirroring Configuration

- Port to Mirror to: The port that will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.
- Ports to Mirror: Select the ports that you want to mirror from this section of the page. A port will be mirrored when the “Mirroring Enabled” check-box is checked.

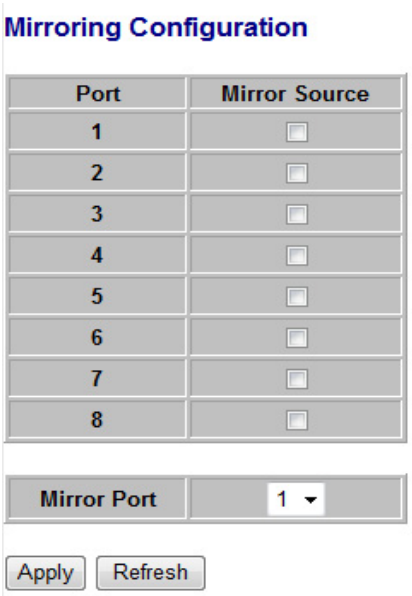


Figure 1-9-1

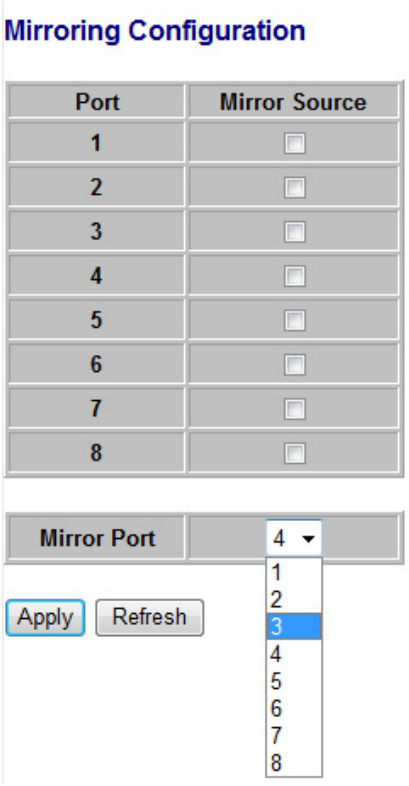


Figure 1-9-2

Quality of Service (QoS)

In QoS Mode, select QoS Disabled, 802.1p, or DSCP to configure the related parameters.

QoS Configuration

- Strict: Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- WRR: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)

  ※Note: WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page.

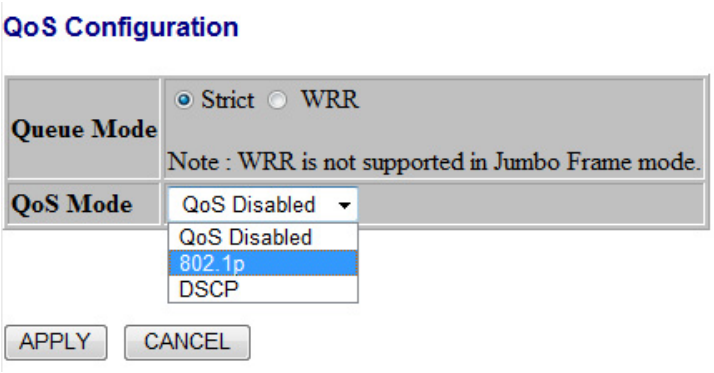


Figure 1-10-1

QoS Mode: QoS Disabled

When the QoS Mode is set to QoS Disabled, the following table is displayed.

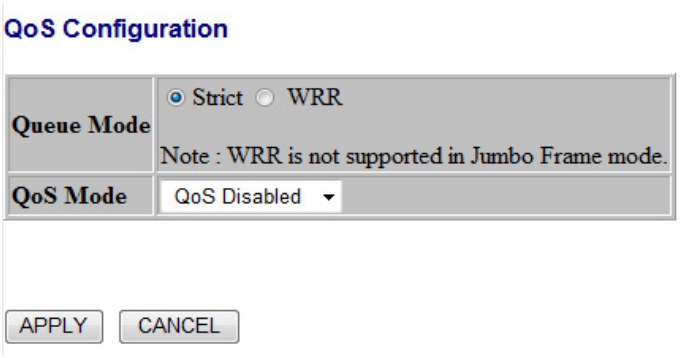


Figure 1-10-2

QoS Mode: 802.1p

Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0 - 7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

When the QoS Mode is set to 802.1p, the 802.1p Configuration table is displayed as shown below.

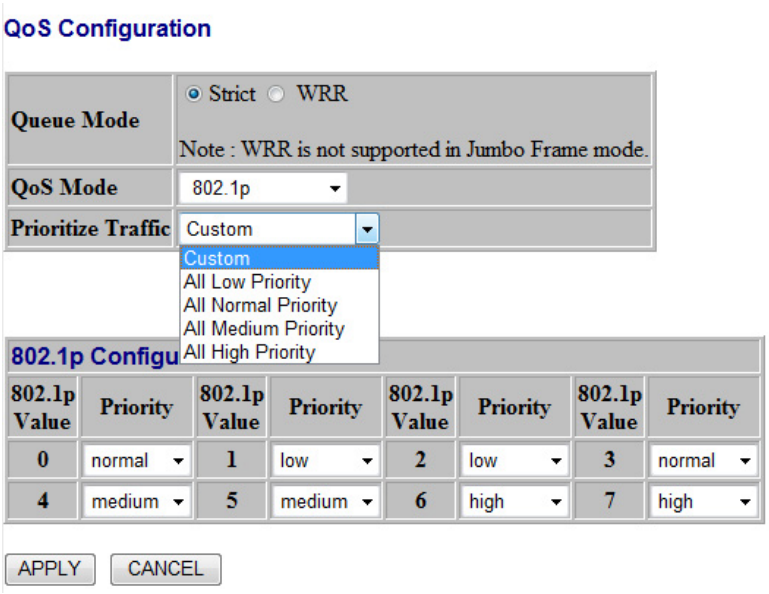


Figure 1-10-3

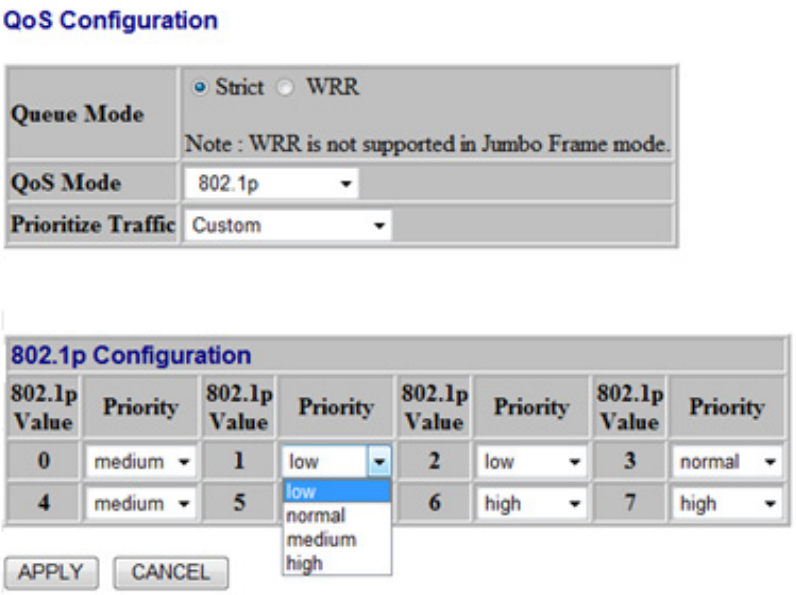


Figure 1-10-4

QoS Mode: DSCP

DSCP: Packets are prioritized using the DSCP (Differentiated Services Code Point) value. The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings map all DSCP values to the high priority egress queue.

User can use the Prioritize Traffic drop-down list to quickly set the values in the

DSCP Configuration table to a common priority queue. Use Custom if you want to set each value individually.

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.

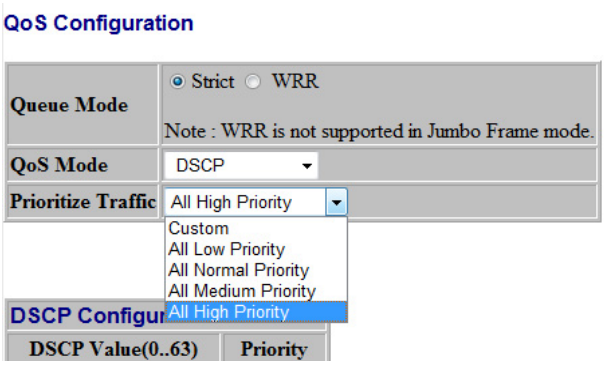


Figure 1-10-5

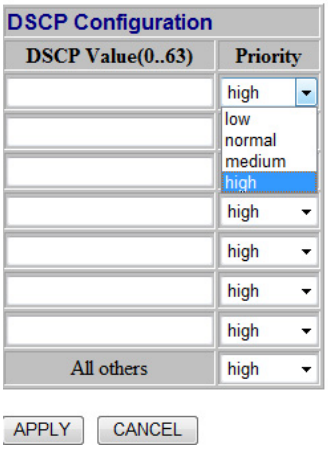


Figure 1-10-6

PoE (Power over Ethernet) Configuration

Power over Ethernet (PoE) is an advanced technology providing a whole new application aspect for networking products. A series of PoE product is powering for wide range of devices, especially useful for VoIP phones, wireless LAN access points and IP cameras.

It is deployed in applications where AC power would be inconvenient, expensive or infeasible to supply. Web Smart features are able to remote control and centralized the power management. Via a current CAT 5 cable, power and data are able to travel though. Not only is it saving costs, but also it meets the demand of energy efficiency.

PoE Configuration

Remote access and monitor the attached PD (Powered Device) status by using Enable/Disable function.

- PoE Enabled: PoE of the port is able to supply power to the attached PD (Powered Device).
- PD Class: Detect the class of PD.
- Delivering Power (W): Output power.
- Current (mA): The status of the port current.
- Voltage (V): The status of the port voltage.
- Power Budget: Total PoE power has been used.

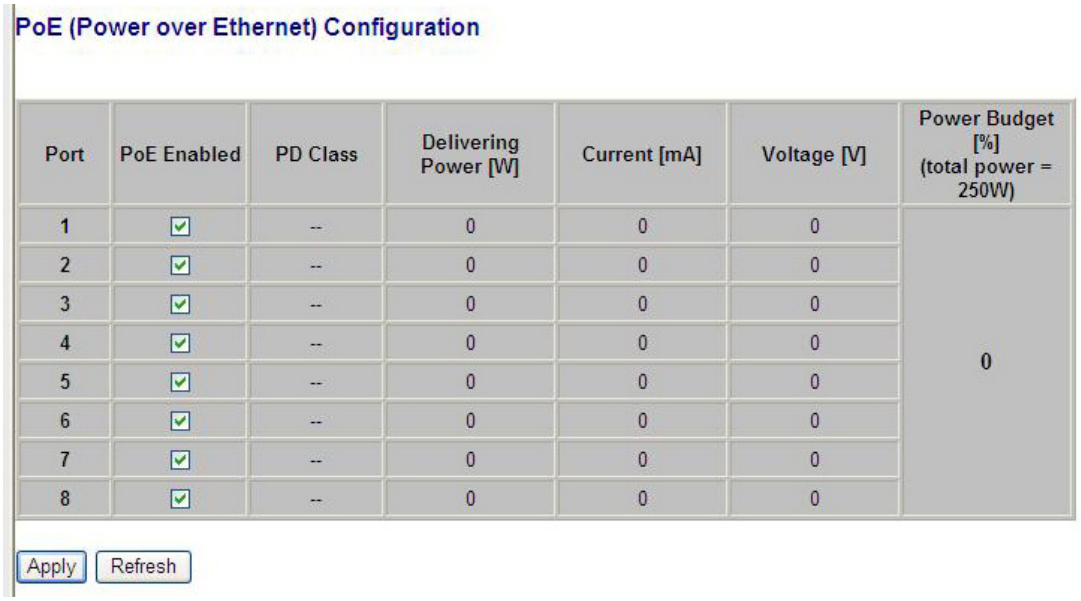


Figure 1-11

Storm Control

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Storm Control Configuration

There are three type of traffic which can be rate limited, including broadcast multicast frame and Flooded Unicast Rate.

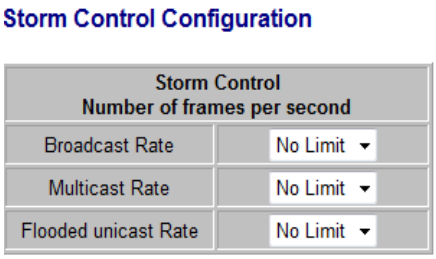


Figure 1-12-1

- Rate (number of frames per second): The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.
- Web: Click Configuration, Storm Control. This page enables you to set the broadcast storm control parameters for every port on the switch.

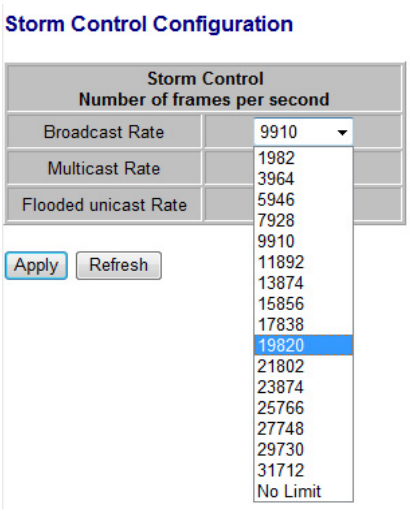


Figure 1-12-2

Monitoring

Statistic Overview

Statistic Overview for all ports

User can mirror traffic from any source port to a target port for real-time analysis the following figures shows clearly the statistics overview.

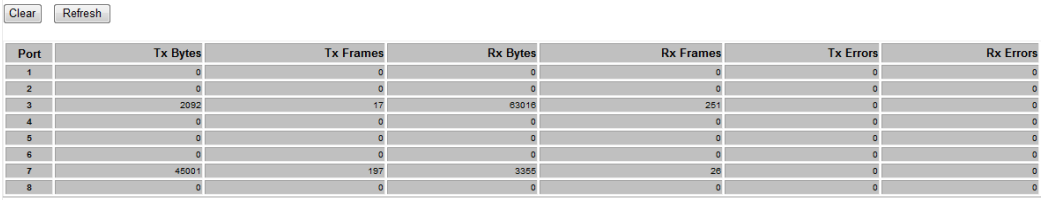
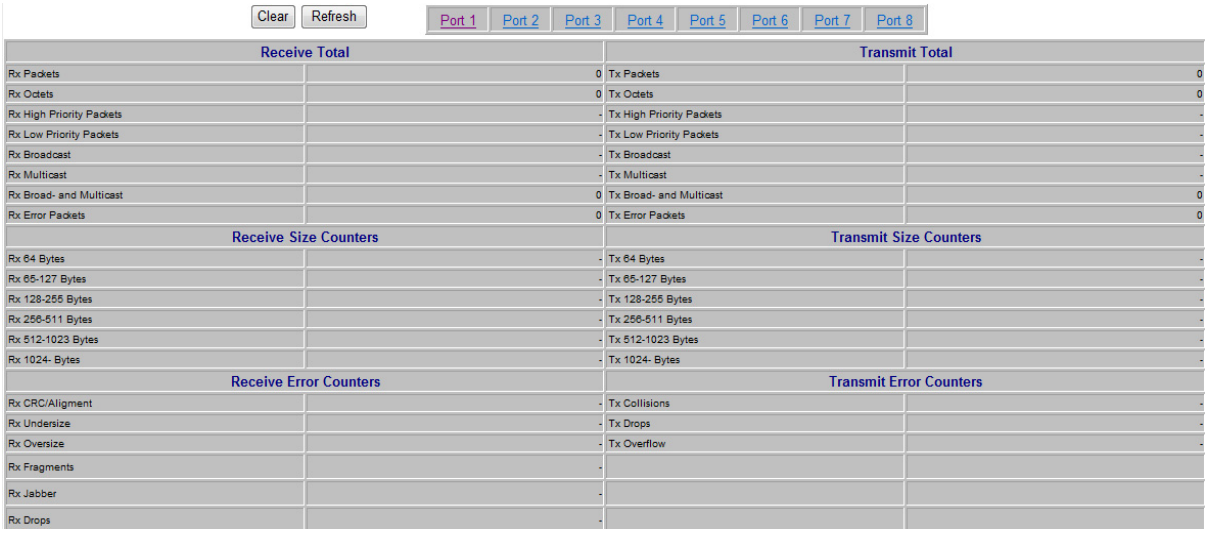


Figure 2-1

Detailed Statics



Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	0	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Figure 2-2

RSTP Status

RSTP VLAN Bridge Overview

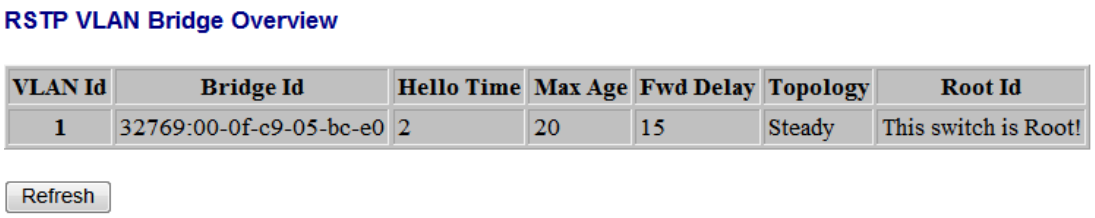
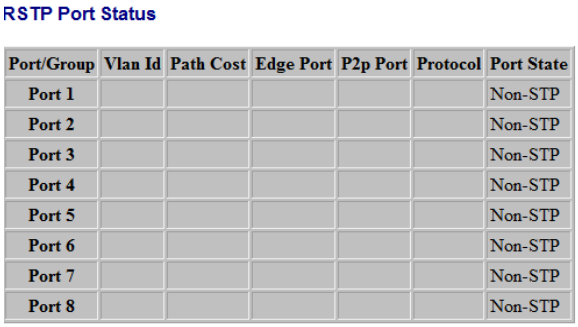


Figure 2-3-1

- Hello Time: Interval (in seconds) at which the root device transmits a configuration message.
- Max Age: The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that age out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.
- Fwd Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- Topology: Indicates if spanning tree topology is steady or undergoing reconfiguration. (The time required for reconfiguration is extremely short, so no values other that “steady” state are likely to be seen in this field.)
- Root ID: The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device, and the port connected to the root device.

RSTP Port Status



RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP

Figure 2-3-2

- Port/Group: The number of a port.
- Vlan Id: Shows Vlan Id of the port.
- Path Cost: The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- Edge Port: Shows if this port is functioning as an edge port, either through manual selection (see the RSTP Port Configuration table) or auto-detection. Note that if the switch detects another bridge connected to this port, the manual setting for Edge Port will be overridden and the port will instead function as a point-to-point connection.
- P2p Port: Shows if this port is functioning as a Point-to-Point connection to exactly one other bridge. The switch can automatically determine if the interface is attached to a point-to-point link or to shared media. If shared media is detected, the switch will assume that it is connected to two or more bridges.
- Protocol: Shows the spanning tree protocol functioning on this port, either RSTP or STP (that is, STP-compatible mode).
- Port State: Shows spanning tree state of the port.

IGMP Status

IGMP Status

IGMP Status shows the IGMP Snooping statistics for the whole switch.

- VLAN ID: VLAN ID number.
- Querier: Show whether Querying is enabled.
- Queries transmitted: Show the number of transmitted Query packets.
- Queries received: Show the number of received Query packets.
- v1 Reports: Show the number of received v1 Report packets.
- v2 Reports: Show the number of received v2 Report packets.
- v3 Reports: Show the number of received v3 Report packets.
- v2 Leave: Show the number of v2 leave packets received.

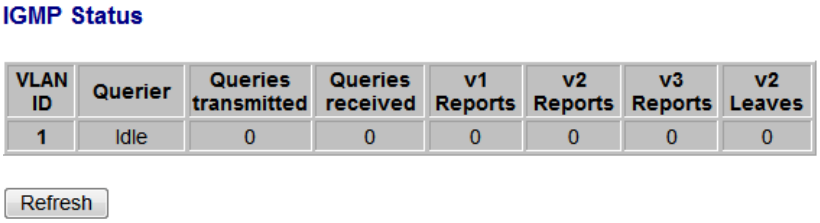


Figure 2-4

Ping

This command sends ICMP echo request packets to another node on the network.

Ping Parameters

- Target IP Address: IP address of the host.
- Count: Number of packets to send. (Range: 1-20)
- Time Out: Setting the time period of host will be Ping.

Use the ping command to see if another site on the network can be reached.
The following are some results of the **ping** command:

- Normal response: The normal response occurs in one to ten seconds, depending on network traffic.
- Destination does not respond: If the host does not respond, a “timeout” appears in ten seconds.
- Destination unreachable: The gateway for this destination indicates that the destination is unreachable.
- Network or host unreachable: The gateway found no corresponding entry in the route table.

Press <Esc> to stop pinging.

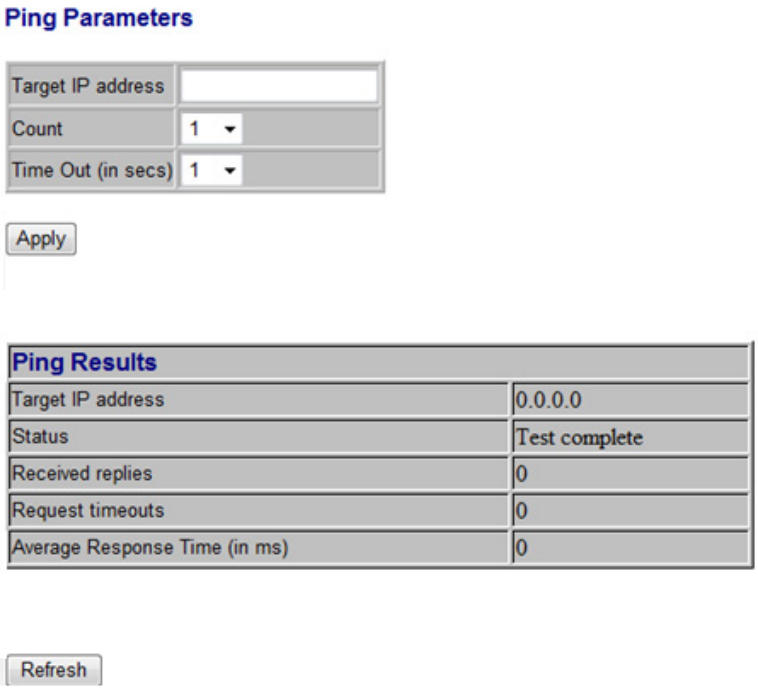


Figure 2-5-1

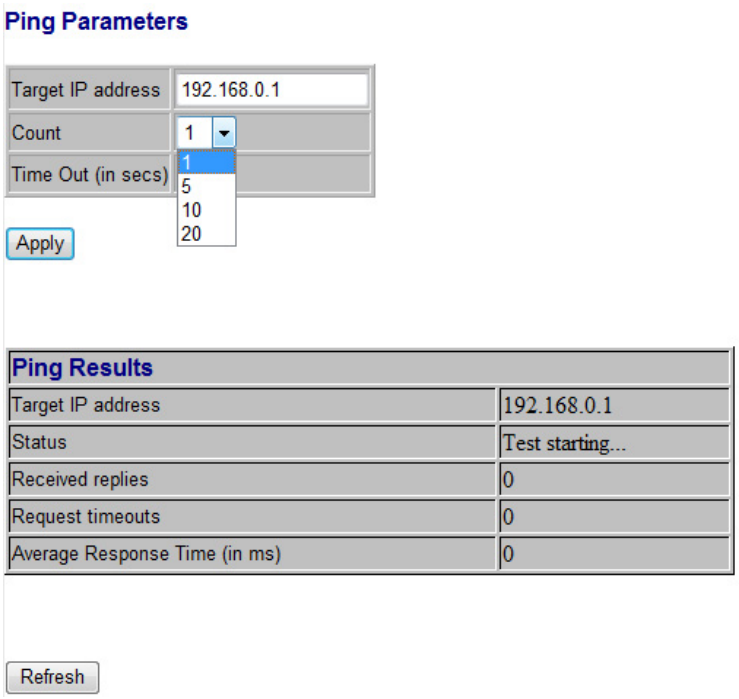


Figure 2-5-2

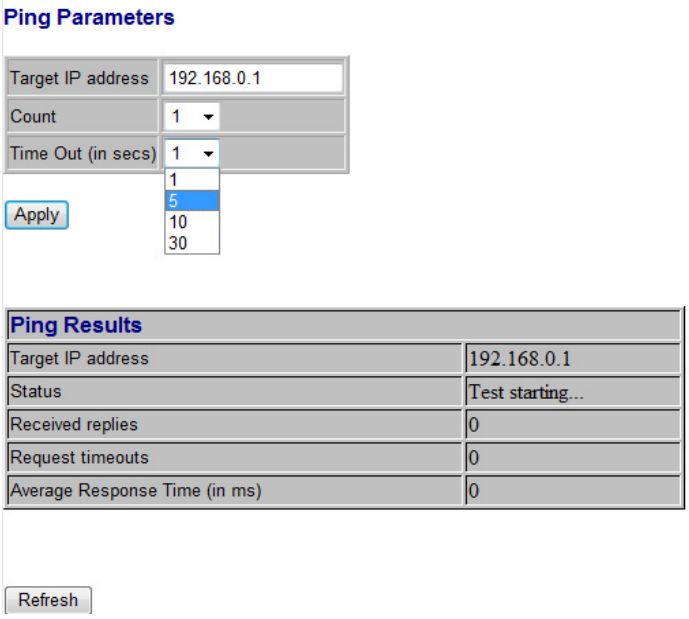


Figure 2-5-3

Maintenance

Warm Restart

Press “Yes” button to restart the switch, the reset will be complete when the power lights stop blinking.

Figure3-1

Factory Default

This function is to force the switch back to the original factory settings. The LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory default.

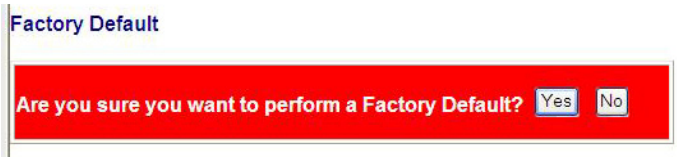


Figure 3-2

Software upload

Select “Software Upload” from the “Maintenance” then click on the “Browse”

button to select the firmware file. Click the “Upload” button to upgrade the selected switch firmware file.

Figure 3-3

Configuration File Transfer

Configuration file transfer allows you to save the switch’s current configuration or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station. “Upload” the configuration file to the device or "Download" to restore a configuration. Use the “Browse” button to choose a file location on the web management station, or to find a saved configuration file.

Figure 3-4

Logout

The administrator has write access for all parameters governing the onboard agent. User should therefore assign a new administrator password as soon as possible, and store it in a safe place.

Figure 3-5

Reset button for the factory default setting

Please take the following steps to reset the Web Smart Switch back to the original default:

Step 1:
Turn on the Web Smart Switch

Step 2:
Press and hold the reset button continuously for 5 seconds and release the reset button.

Step 3:
The switch will reboot for 20 seconds and the configuration of switch will back to the default setting.